

THE UNIVERSITY of EDINBURGH
informatics

Introduction to Quantum Computing

Lecture 18: Quantum Phase Estimation

Raul Garcia-Patron Sanchez



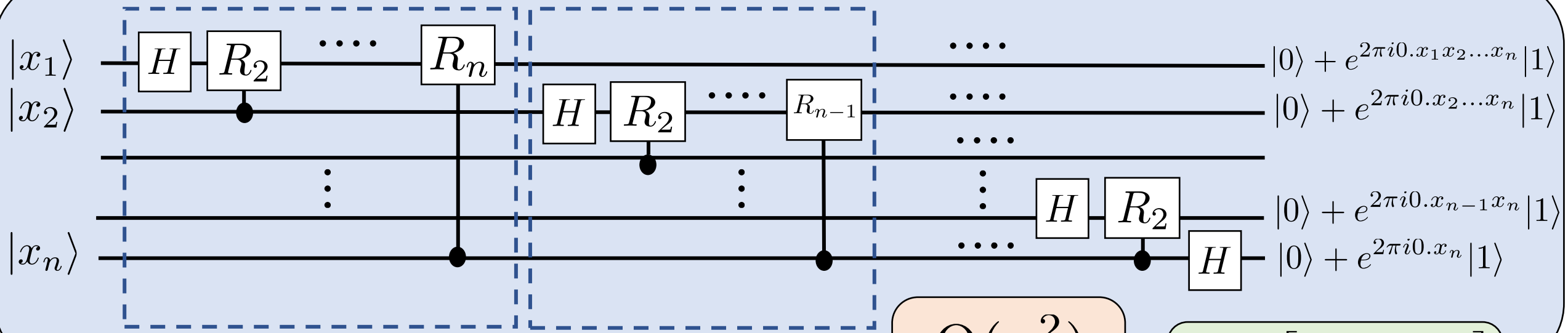
Recap Fourier Transform

Quantum Fourier Transform over $\mathbb{Z}_{2^n}$

Binary representation: $z = z_1 2^{n-1} + z_2 2^{n-2} + ... + z_{n-1} 2 + z_n$

Binary fraction: $0.w_l w_{l+1} \ldots w_m = \frac{w_l}{2} + \frac{w_{l+1}}{2^2} + \cdots + \frac{w_m}{2^{m-l+1}}$

$$|x_1, x_2, ..., x_{n-1}, x_n\rangle \to \frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.x_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.x_2 ... x_n}|1\rangle)(|0\rangle + e^{2\pi i 0.x_1 x_2 ... x_n}|1\rangle)$$



$\Theta(n^2)$ gates

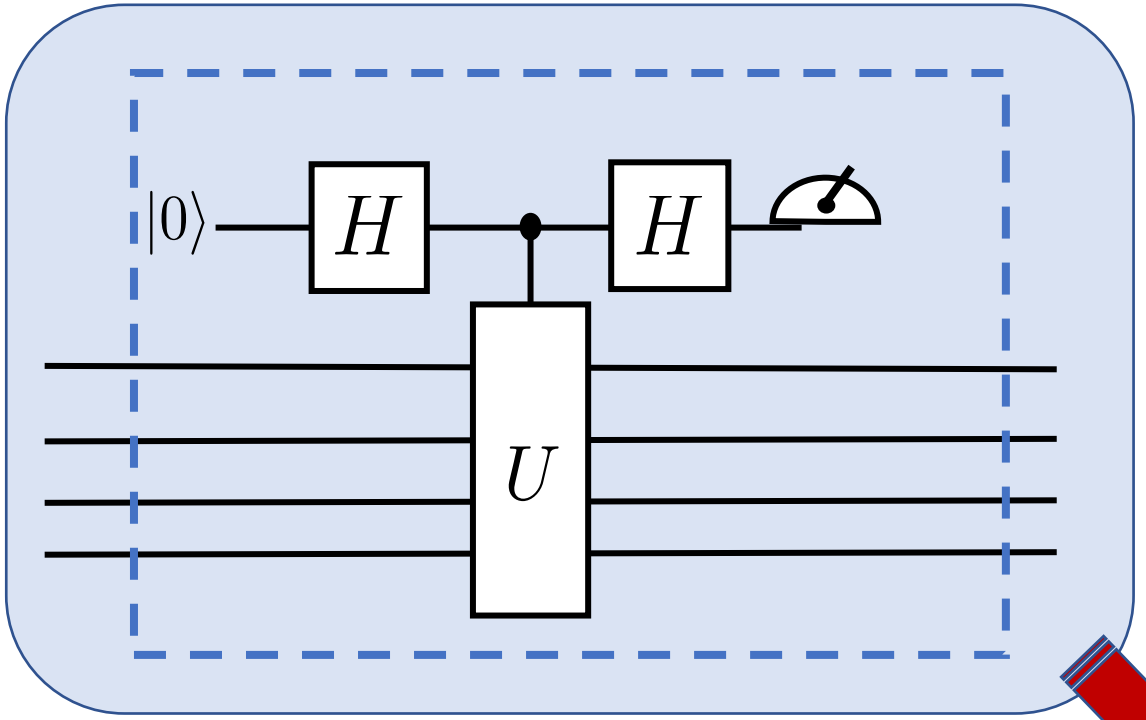
$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{bmatrix}$$

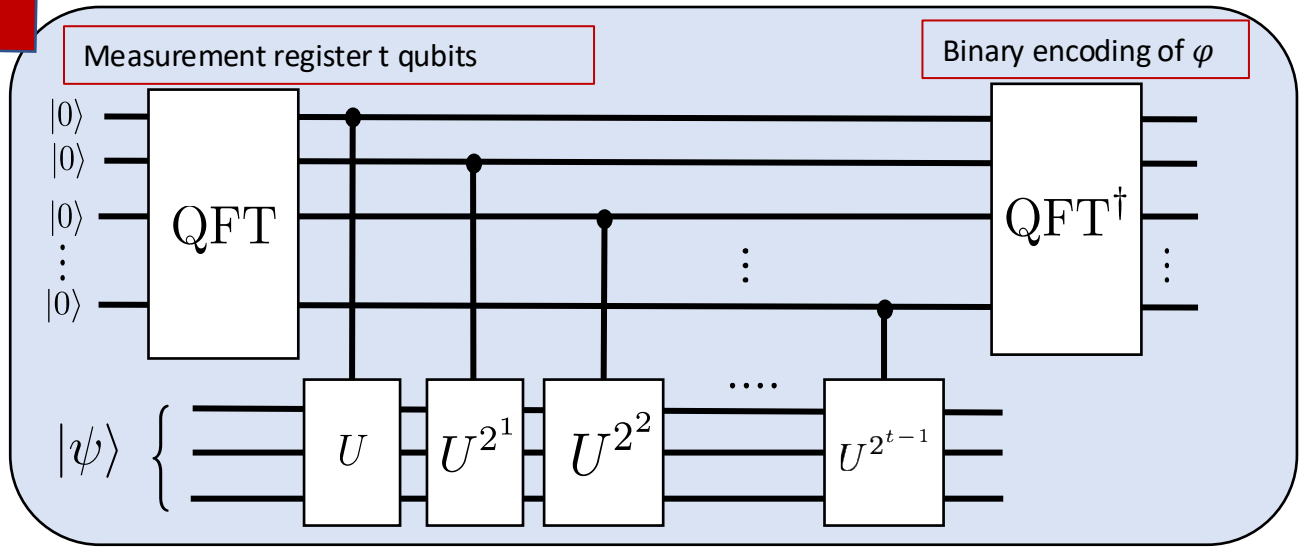


THE UNIVERSITY of EDINBURGH
informatics

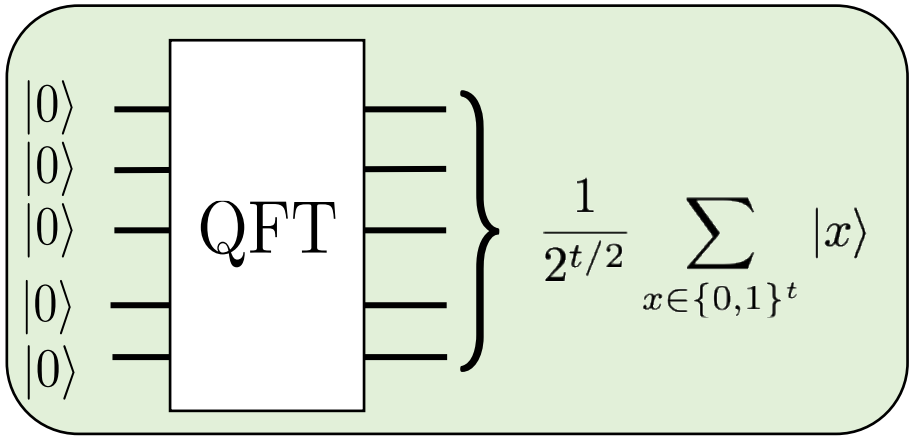
Quantum phase estimation

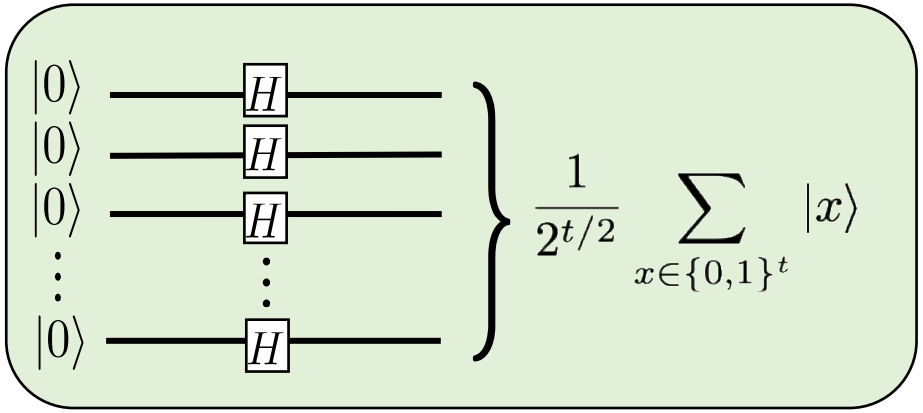
Generalization to multiple-outcome measurement

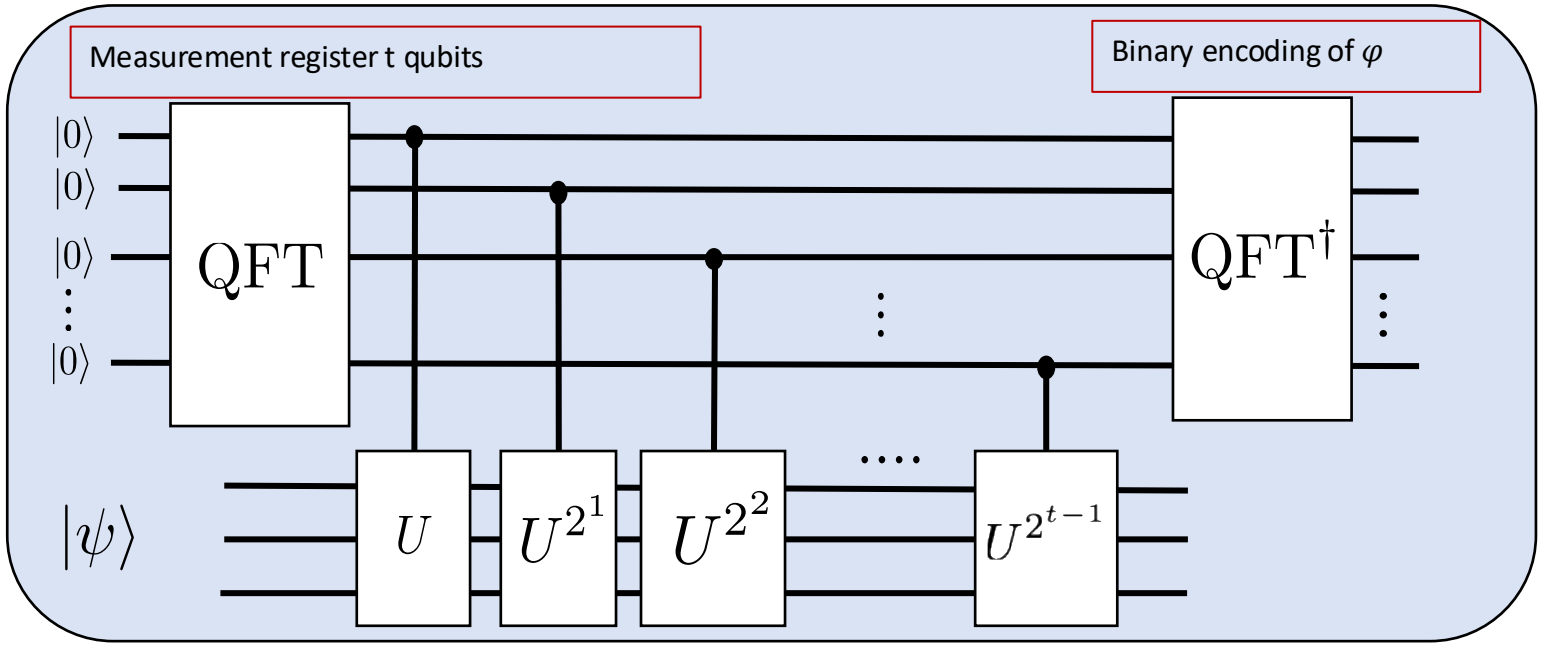


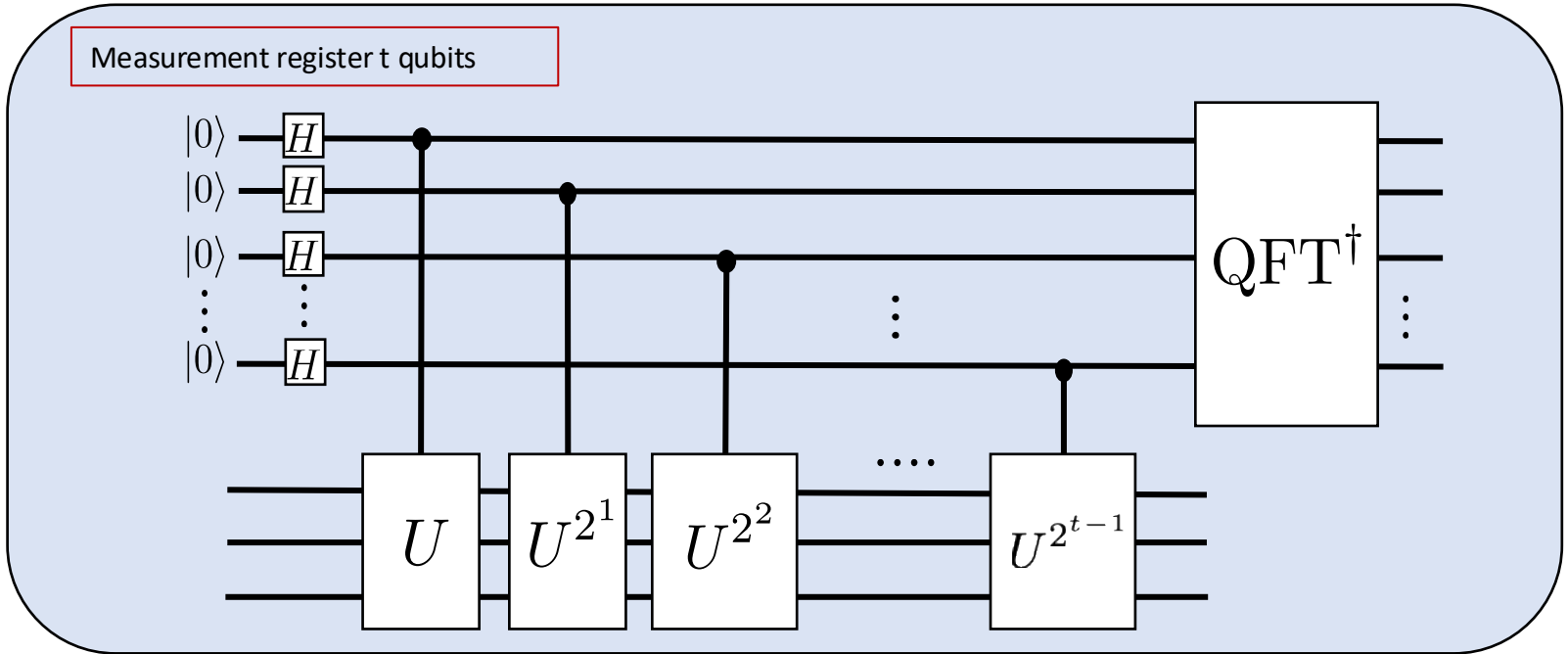


Quantum phase estimation: applications









The eigenspace and eigenvalues of unitary matrices

Spectral theorem

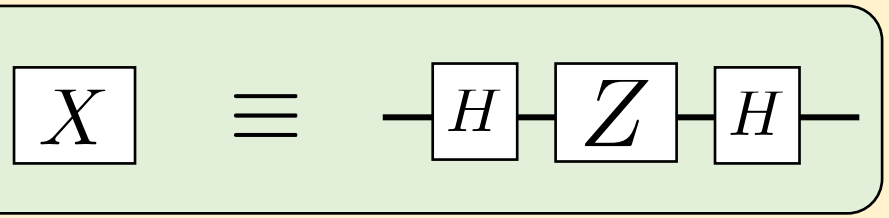
Normal matrix $A : AA^\dagger = A^\dagger A$

$$\exists V : VAV^\dagger = D = \mathrm{diag}(\lambda_1, \ldots, \lambda_N)$$

$$A = \sum_{i=1}^{N} \lambda_i |u_i\rangle\langle u_i|, \text{ and } V = \sum_{i=1}^{N} |i\rangle\langle u_i|$$

Unitary $U : UU^\dagger = U^\dagger U = I$

$$\exists V : VUV^\dagger = D = \mathrm{diag}(e^{2\pi i\varphi_1}, ..., e^{2\pi i\varphi_N})$$



- N eigenvalues on the unit circle: $\lambda_i = e^{2\pi i\varphi_i}$
- $U = \sum_{i=1}^{N} e^{2\pi i\varphi_i} |u_i\rangle\langle u_i|$, and $V = \sum_{i=1}^{N} |i\rangle\langle u_i|$ $\quad \{|u_i\rangle\}$ is an orthonormal basis

Degeneracy

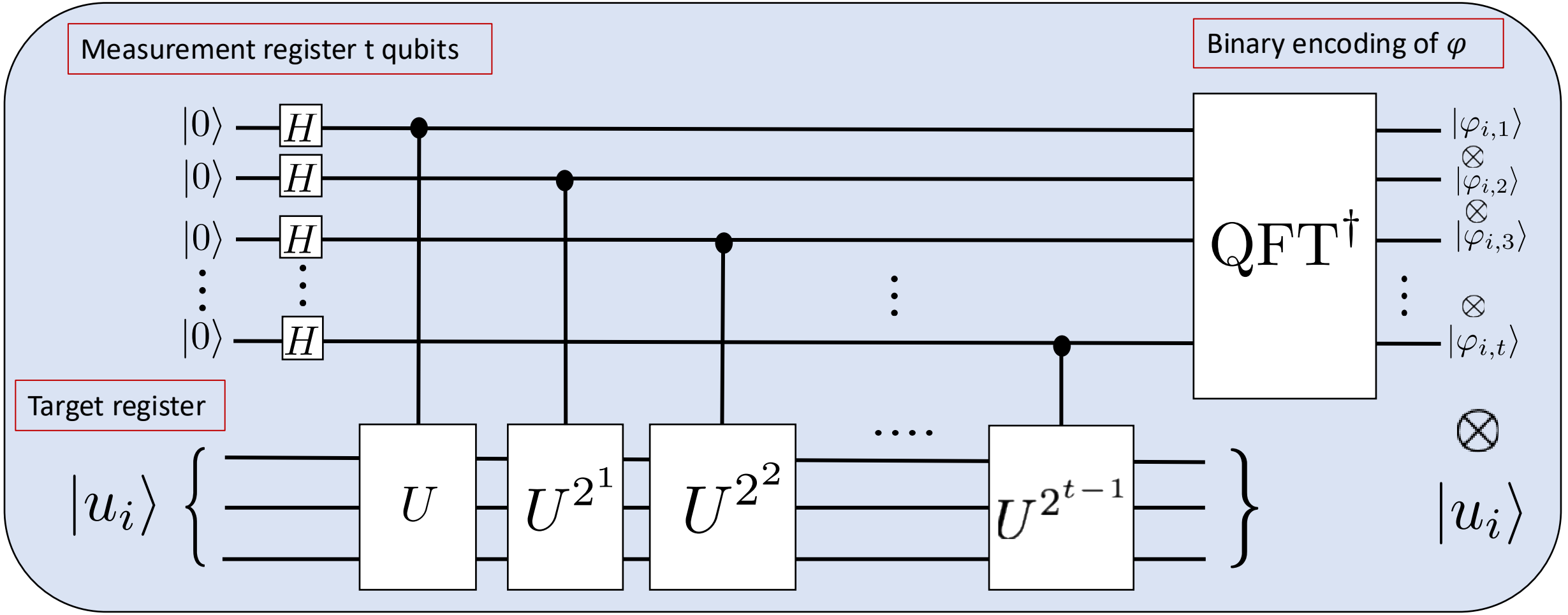
Build projectors as sum of eigenvectors with same eigenvalue.

$$\Pi_i = \sum_{k:\varphi_k=\varphi_i} |u_k\rangle\langle u_k| \qquad U = \sum_{i=1}^{L} e^{2\pi i\varphi_i} \Pi_i$$

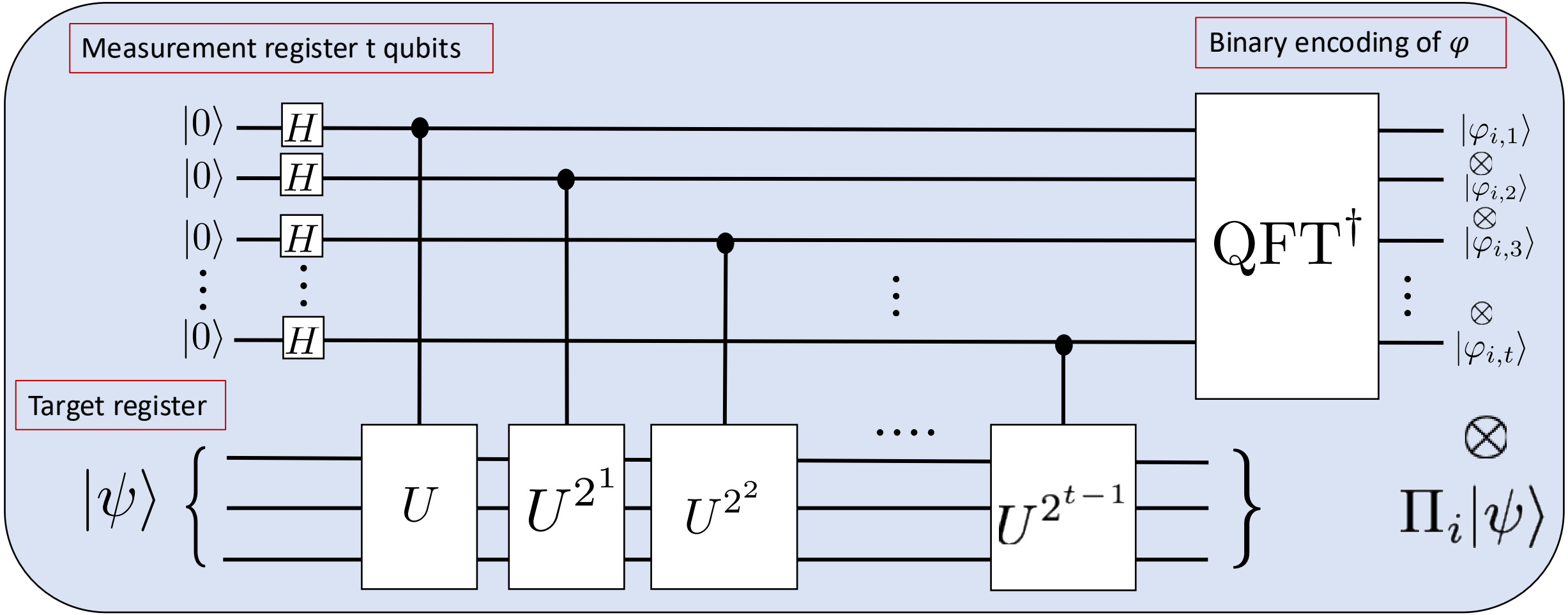
Quantum phase estimation

Projective measurement on the basis $|u_i\rangle$ with outcome $\varphi_i \in [0, 1)$

Assumptions:
- We can perform the controlled-U^{2^j} operation
- All φ_i have at most t digits in binary encoding



Quantum phase estimation



$$|0^t\rangle \otimes |\psi\rangle = |0^t\rangle \otimes (\sum_i \Pi_i|\psi\rangle) = \sum_i |0^t\rangle \otimes \Pi_i|\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes \Pi_i|\psi\rangle$$

- Π_i is projector on subspace of eigenvalue $e^{2\pi i\varphi_i}$
- With probability $||\Pi_i|\psi\rangle||^2$ the measurement outputs $|\varphi_i\rangle$

General ± 1 eigenvalues measurement

QPE

$$|0^t\rangle \otimes |\psi\rangle = |0^t\rangle \otimes (\sum_i \Pi_i |\psi\rangle) = \sum_i |0^t\rangle \otimes \Pi_i |\psi\rangle \to \sum_i |\varphi_i\rangle \otimes \Pi_i |\psi\rangle$$

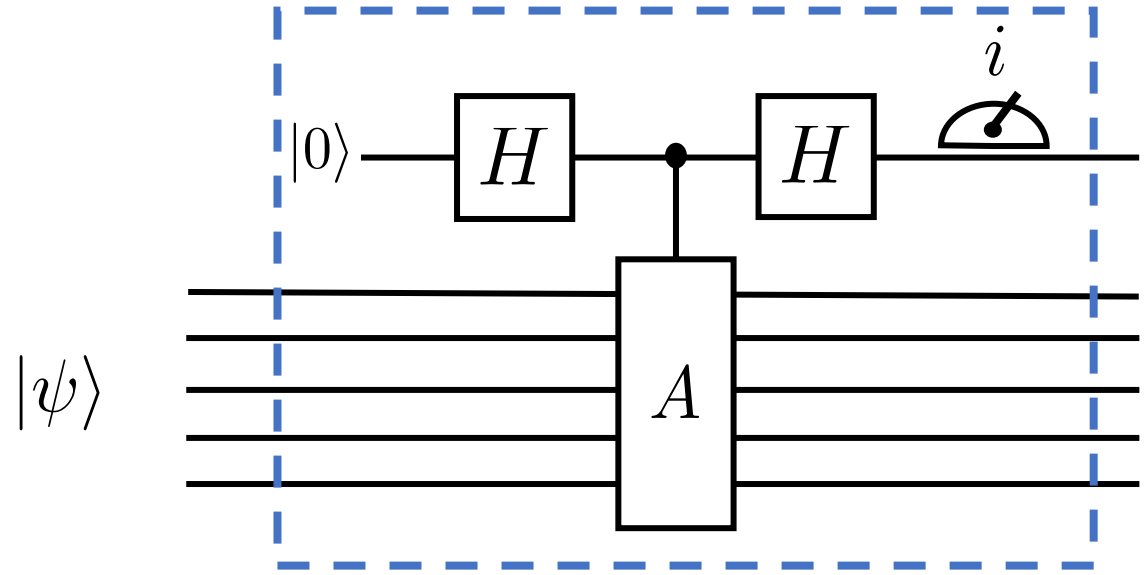
- Π_i is projector on subspace of eigenvalue $e^{2\pi i \varphi_i}$
- With probability $||\Pi_i|\psi\rangle||^2$ the measurement outputs $|\varphi_i\rangle$

Hadamard test

$$\Pi_0 + \Pi_1 = I$$

$$A = \Pi_0 - \Pi_1$$

$$A\Pi_x = (-1)^x \Pi_x$$



Hadamard test is QPE with binary outcome

$$|\tilde{\phi}\rangle = |0\rangle \otimes \Pi_0 |\psi\rangle + |1\rangle \otimes \Pi_1 |\psi\rangle$$

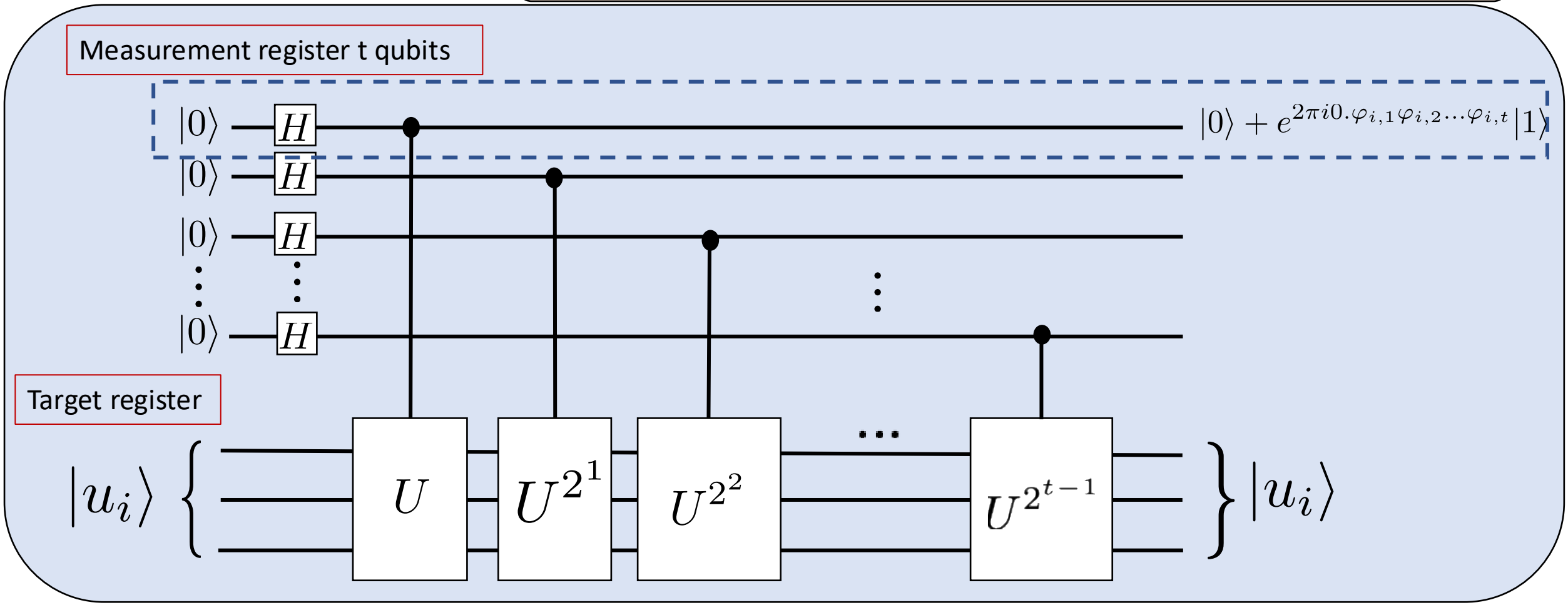
$$(-1)^z = e^{\pi i z} = e^{2\pi i 0.z} \text{ where } z \in \{0, 1\}$$

Quantum phase estimation: Proof

$$\varphi_i \in [0,1)$$
$$U|u_i\rangle = e^{2\pi i\varphi_i}|u_i\rangle$$

$$\varphi_i = 0.\varphi_{i,1}\varphi_{i,2}\dots\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + \dots + \frac{\varphi_{i,t}}{2^t}$$

$$(|0\rangle + |1\rangle) \otimes |u_i\rangle \rightarrow (|0\rangle + e^{2\pi i\varphi_i}|1\rangle) \otimes |u_i\rangle$$



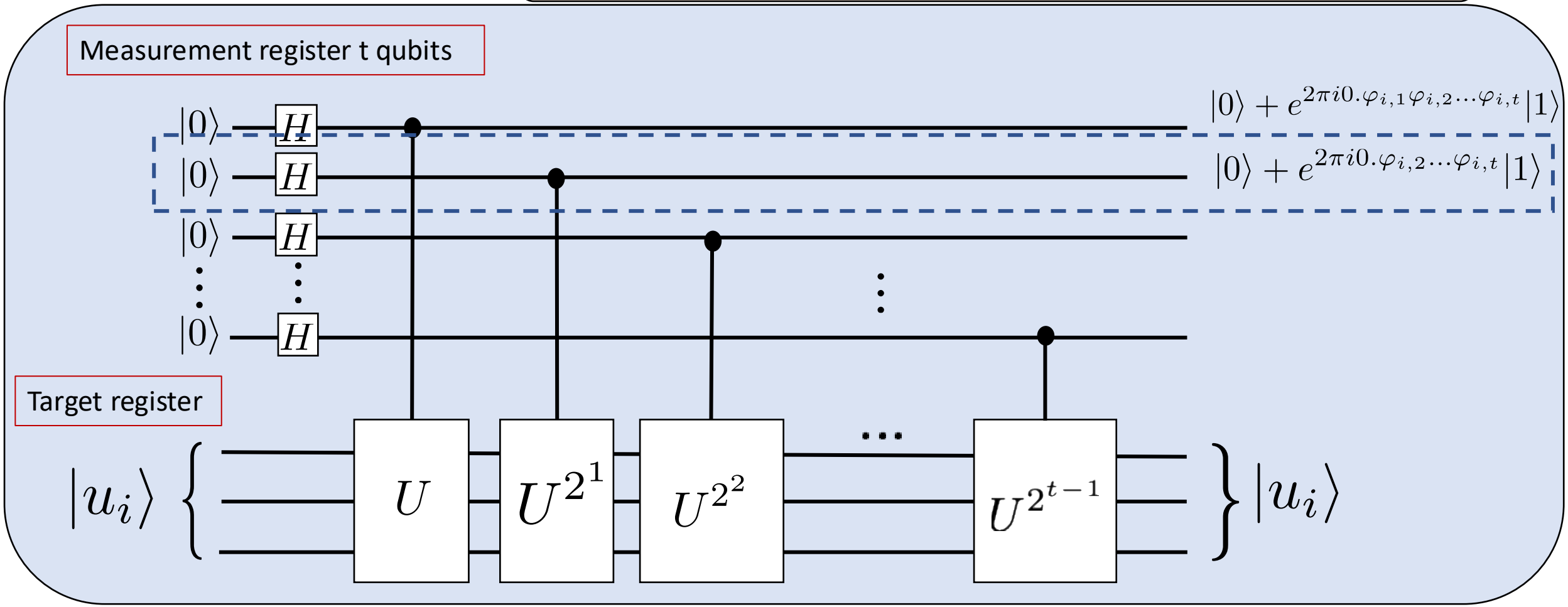
Quantum phase estimation: Proof

$$U|u_i\rangle = e^{2\pi i\varphi_i}|u_i\rangle$$
$$U^{2^k}|u_i\rangle = e^{2\pi i 2^k\varphi_i}|u_i\rangle$$

$$2\varphi_i = \varphi_{i,1} + \frac{\varphi_{i,2}}{2} + \ldots + \frac{\varphi_{i,t}}{2^{t-1}}$$

$$|0\rangle + e^{2\pi i 2\varphi_i}|1\rangle = |0\rangle + e^{2\pi i 0.\varphi_{i,2}\ldots\varphi_{i,t}}|1\rangle$$

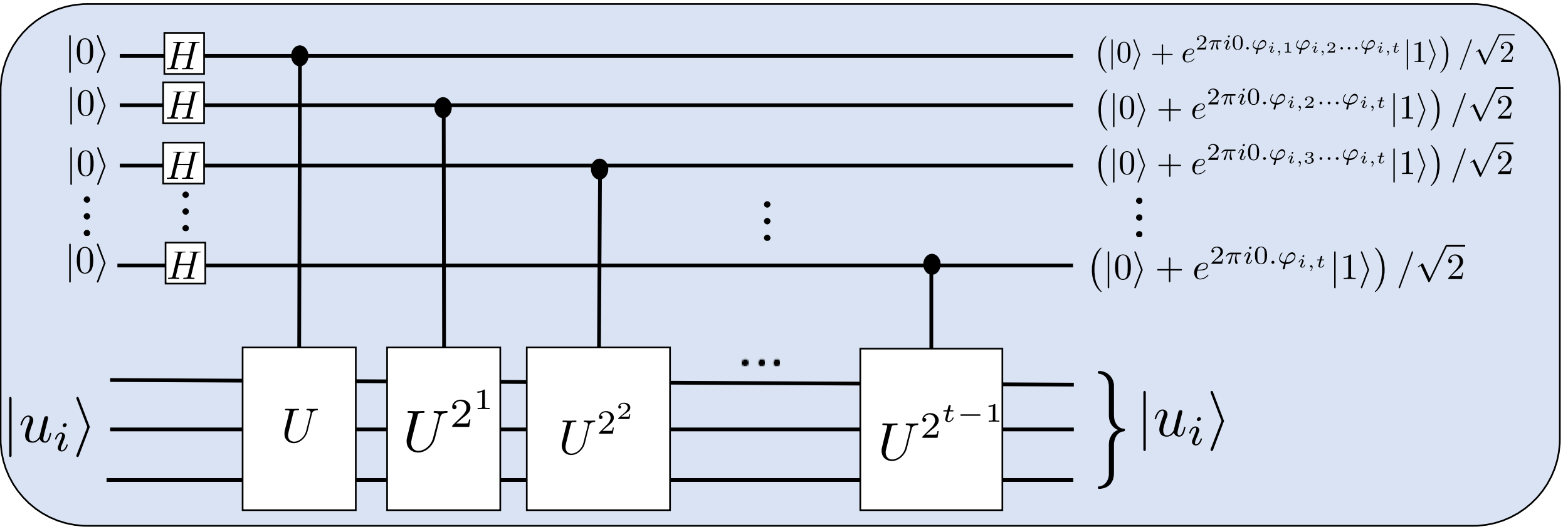
Measurement register t qubits



Quantum phase estimation: Proof

$$\varphi_i \in [0,1) \qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}\dots\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + \dots + \frac{\varphi_{i,t}}{2^t}$$

$$e^{2\pi i 2^k \varphi} = e^{2\pi i (2^{k-1}\varphi_{i,1} + \dots + \varphi_{i,k})} e^{2\pi i 0.\varphi_{i,k+1}\dots\varphi_{i,t}} = e^{2\pi i 0.\varphi_{i,k+1}\dots\varphi_{i,t}}$$

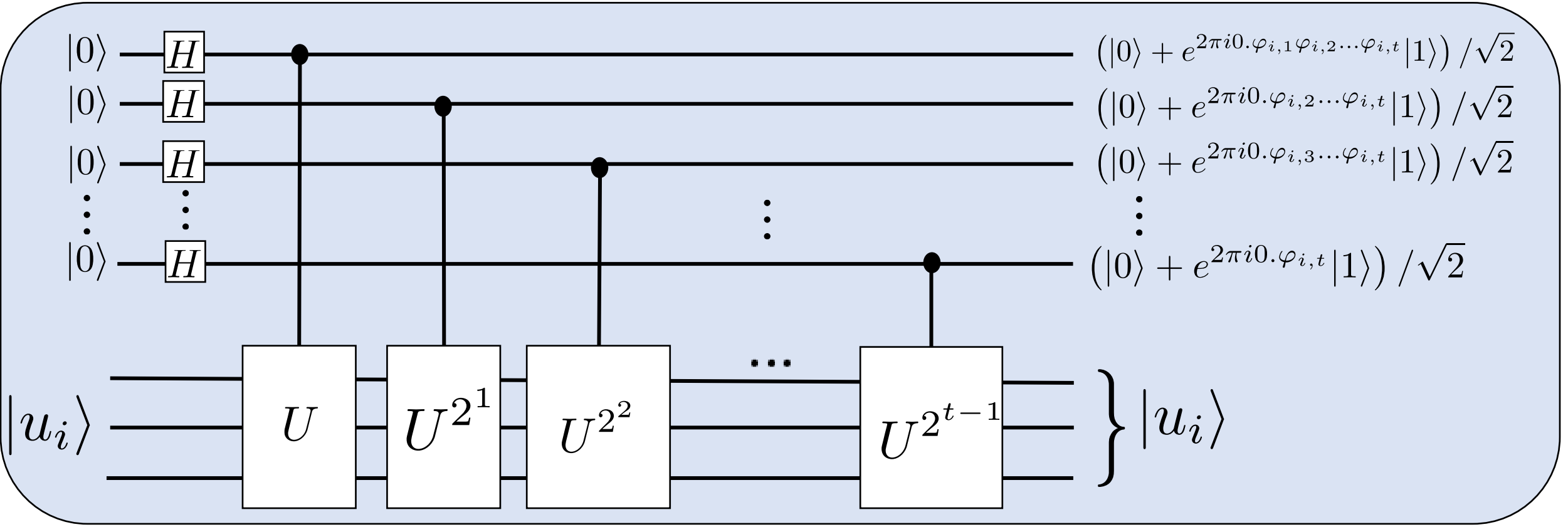


Quantum phase estimation: Proof

$$\varphi_i \in [0,1) \qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}\dots\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + \dots + \frac{\varphi_{i,t}}{2^t}$$

$$|x_1, x_2, \dots, x_{t-1}, x_t\rangle \rightarrow \frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.x_t}|1\rangle)(|0\rangle + e^{2\pi i 0.x_{t-1}x_t}|1\rangle)\dots(|0\rangle + e^{2\pi i 0.x_1 x_2 \dots x_t}|1\rangle)$$

QFT

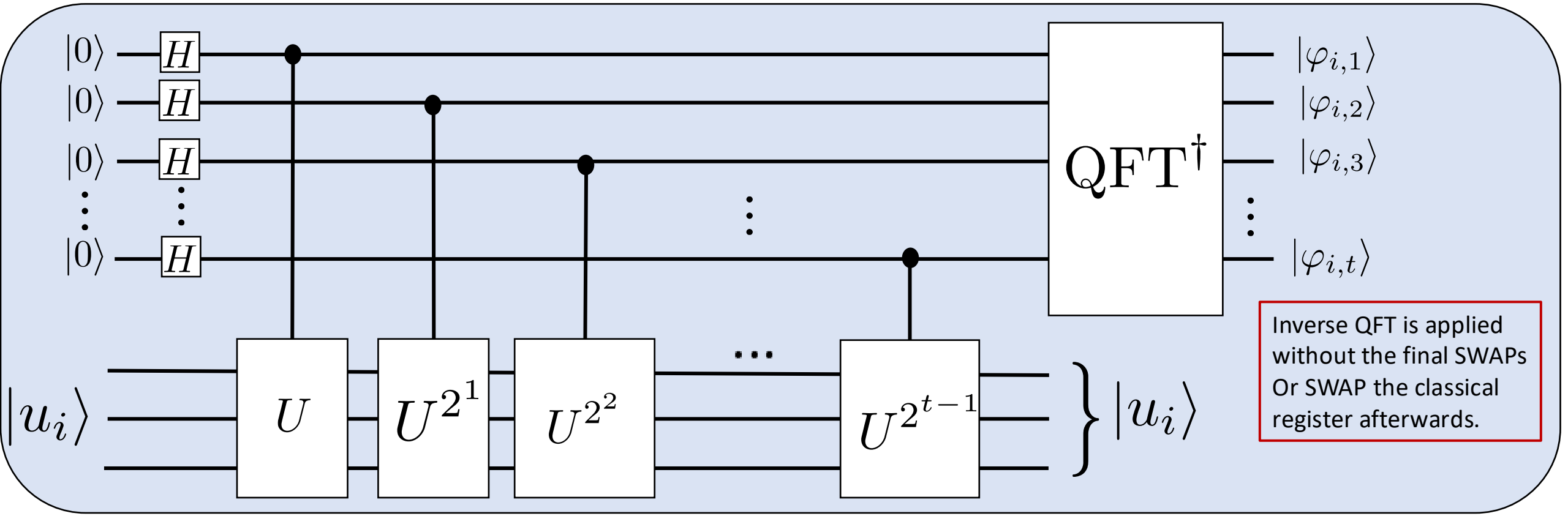


Quantum phase estimation: Proof

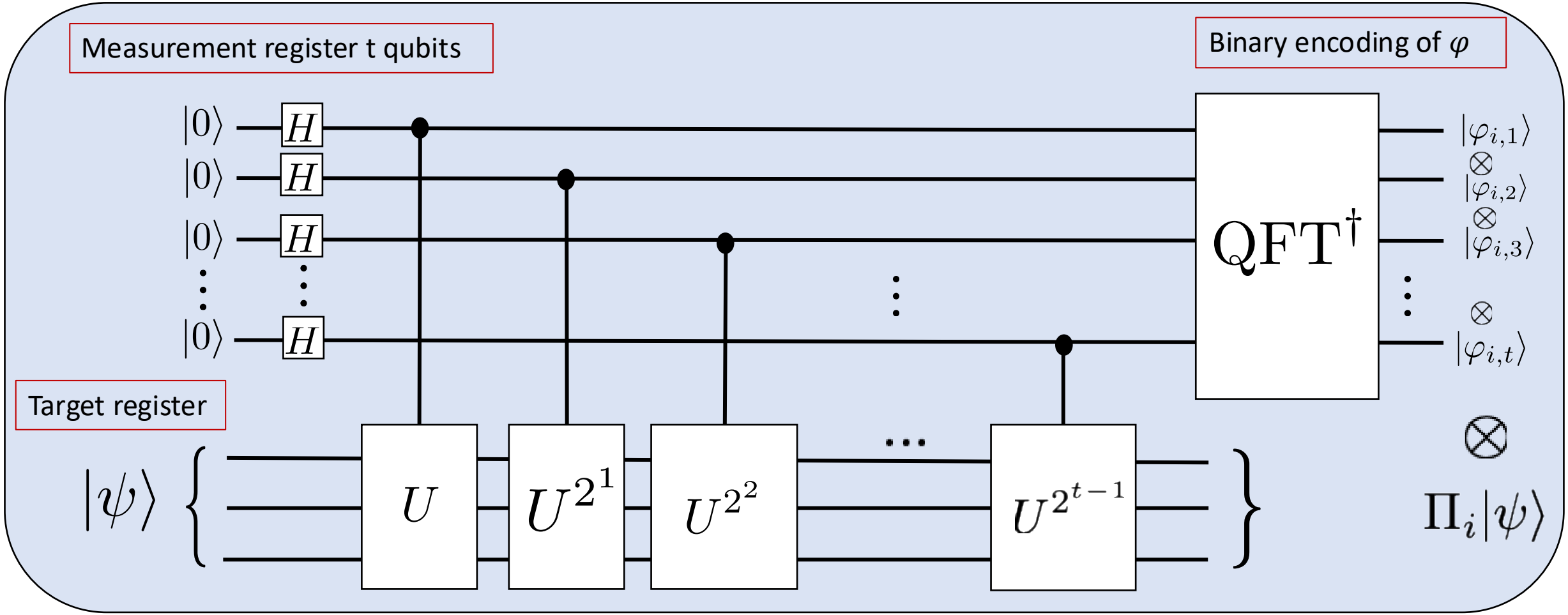
$$\varphi_i \in [0,1) \qquad \varphi_i = 0.\varphi_{i,1}\varphi_{i,2}\dots\varphi_{i,t} = \frac{\varphi_{i,1}}{2} + \frac{\varphi_{i,2}}{2^2} + \dots + \frac{\varphi_{i,t}}{2^t}$$

$$|x_1, x_2, \dots, x_{t-1}, x_t\rangle \rightarrow \frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.x_t}|1\rangle)(|0\rangle + e^{2\pi i 0.x_{t-1}x_t}|1\rangle)\dots(|0\rangle + e^{2\pi i 0.x_1 x_2 \dots x_t}|1\rangle)$$

QFT



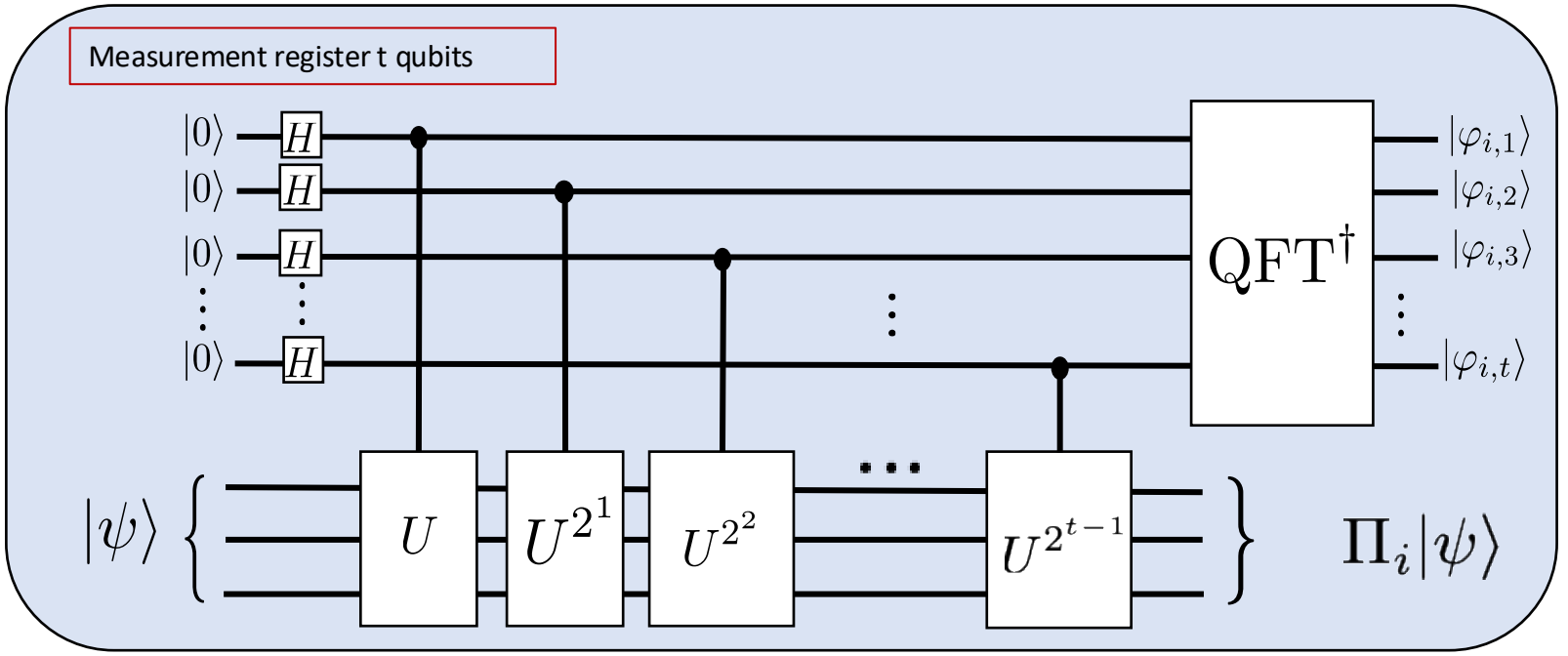
Quantum phase estimation



- $$|0^t\rangle \otimes |\psi\rangle = |0^t\rangle \otimes (\sum_i \Pi_i|\psi\rangle) = \sum_i |0^t\rangle \otimes \Pi_i|\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes \Pi_i|\psi\rangle$$
- Π_i is projector on subspace of eigenvalue $e^{2\pi i\varphi_i}$
- With probability $||\Pi_i|\psi\rangle||^2$ the measurement outputs $|\varphi_i\rangle$

Application and Discussion

$$|0^t\rangle \otimes |\psi\rangle \rightarrow \sum_i |\varphi_i\rangle \otimes \Pi_i |\psi\rangle$$



- Can we implement U^{2^k} efficiently?
  - Sometimes YES!!, see Shor's algorithm.
  - Most of the time not! or we could exp-accelerate quantum simulation.
- To obtain φ with n-bit accuracy with probability of error ϵ
  - we need to satisfy: $t = n + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$



THE UNIVERSITY of EDINBURGH
informatics

Shor algorithm:

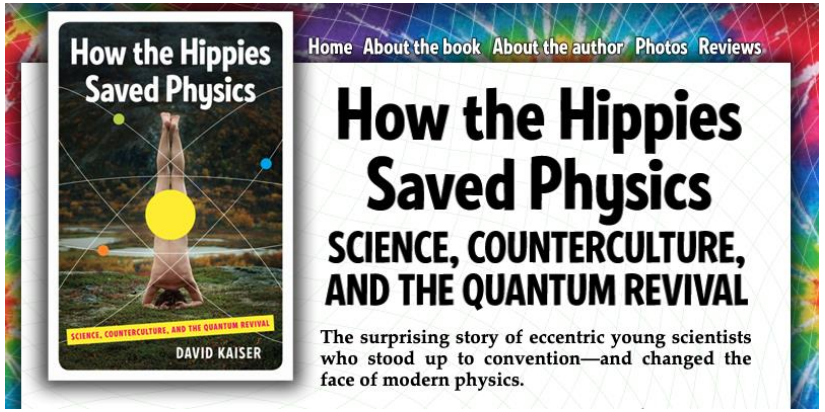
QPE for modular exponentiation

Shor's Algorithm for Factoring

Input: $N \in \mathbb{N}$. An integer with n-bit binary encoding.
Promise: $N = p_1 p_2$ where p_1, p_2 are distinct odd primes.
Problem: find p_1 and p_2

- Major breakthrough in 1994

Classical: $\exp(O(n^{1/3} \log^{2/3} n))$
Quantum: $O(n^3)$



- Changed the field of quantum computation

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Summary Factoring

$N = p_1 \cdot p_2$

- Pick $\kappa \in \mathbb{N} : 1 < \kappa < N$ at random.
- Compute $GCD(\kappa, N)$ using Euclid's Algorithm.

$$\text{If } GCD(\kappa, N) \neq 1 \Rightarrow GCD(\kappa, N) = p_1 \text{ or } p_2$$

As unlikely as random guessing 

$$f_{N,\kappa}(x) = \kappa^x \pmod N \quad \text{Least positive } r : \kappa^r \pmod N = 1$$

- We call ORDER FINDING to obtain r.
- $\text{GCD}(\kappa^{r/2} - 1, N) = p_1 \quad \text{GCD}(\kappa^{r/2} + 1, N) = p_2$

H1 r is even: $r/2 \in \mathbb{N}$. H2 $\kappa^{r/2} + 1 \neq 0 \pmod N$

- We have a verification of solution. $P\left[\kappa < N : \text{H1} \cap \text{H2}\right] \geq 1/2$

THE UNIVERSITY of EDINBURGH
informatics



Order finding

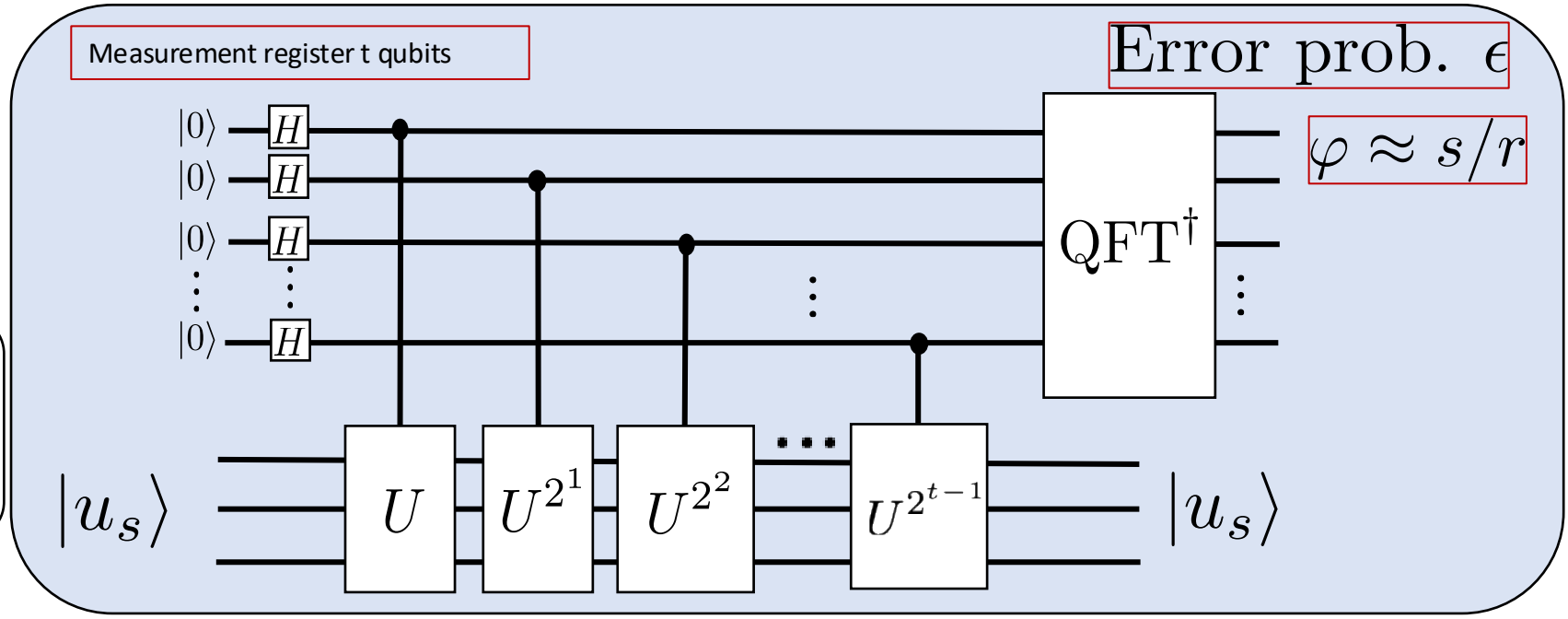
Phase estimation for order finding

$$U|y\rangle \equiv |\kappa y \pmod N\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$

Binary encoding of N

$L \equiv \lceil \log(N) \rceil$



- $|u_s\rangle$ is eigenvector of U of eigenvalue $e^{2\pi i s/r}$ with $s \in \{0, \ldots, r-1\}$

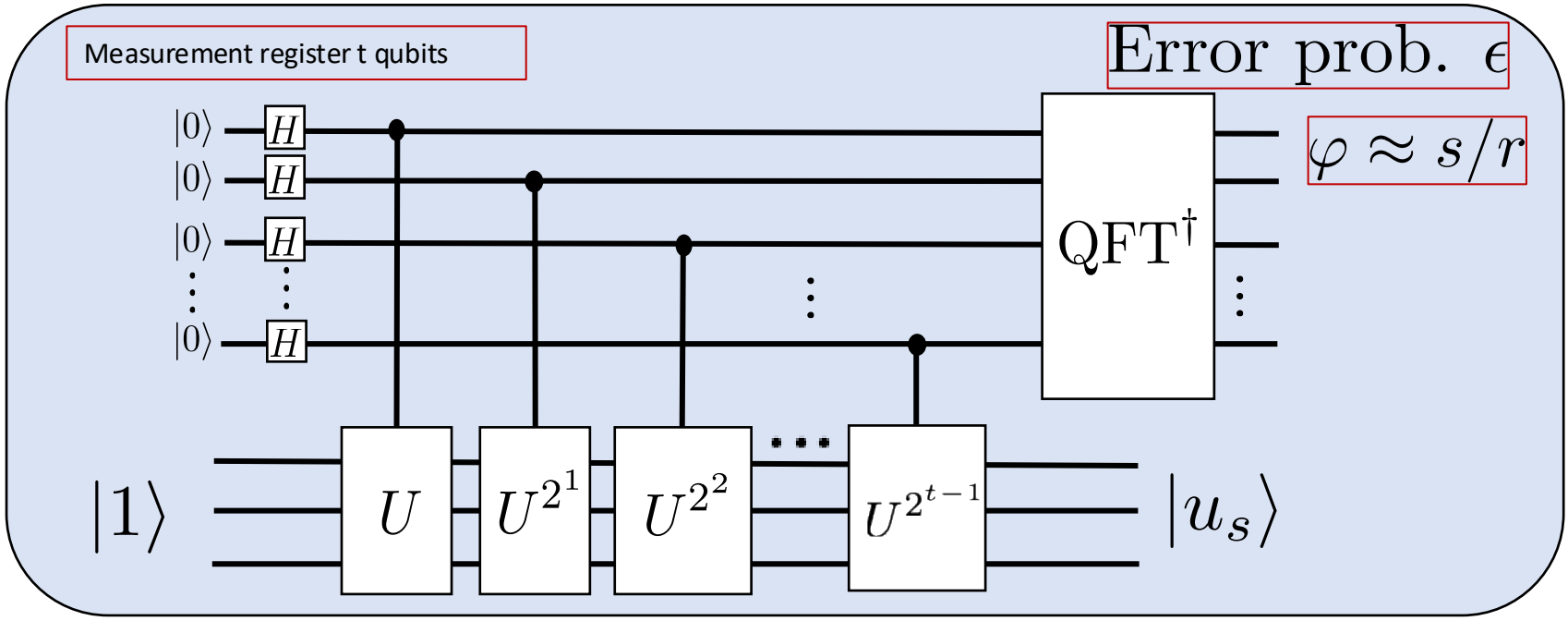
$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} e^{-2\pi i s l/r} |\kappa^l \pmod N\rangle \quad U|u_s\rangle = e^{2\pi i s/r}|u_s\rangle$$

- Continued fractions extract s/r from φ
- Approximation φ of $2L+1$ bits, if $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$

The input state

$$U|y\rangle \equiv |\kappa y \pmod N\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$



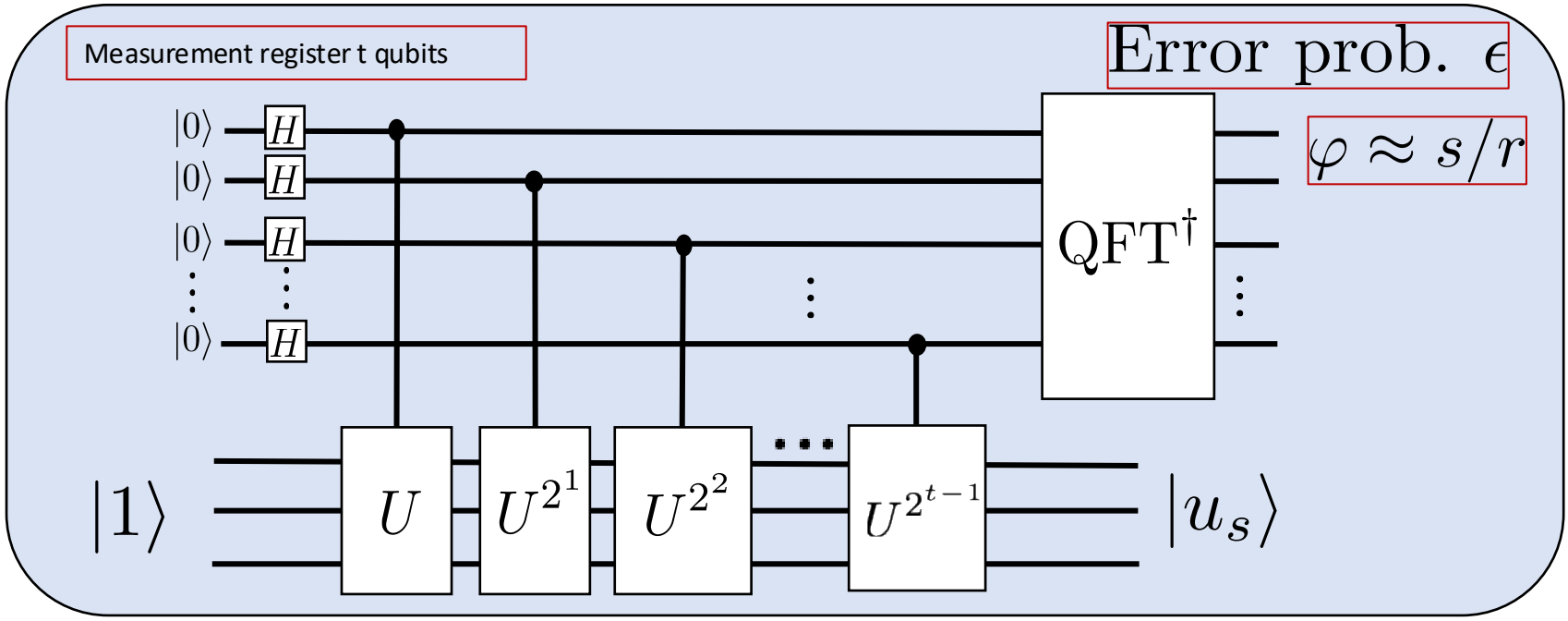
- $|u_s\rangle$ is eigenvector of U of eigenvalue $e^{2\pi i s/r}$
- But to generate $|u_s\rangle$ we need to know r.

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle = |0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle$$

Post-processing: potential error

$$U|y\rangle \equiv |\kappa y \pmod N\rangle$$

Unitary as $\mathrm{GCD}(\kappa, N) = 1$



- Continued fractions returns s/r in lowest terms s'/r'
- If GCD $(s, r) \neq 1$ we get $r' < r$ (a divisor of r)
  - For random $s \in \{0, \ldots, r-1\}$ high prob. $\mathrm{GCD}(s, r) = 1$

#co-primes: $\Omega(r/\log\log r) \Rightarrow$ repeat $O(\log L)$

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$$

References

Reading references

1. Phase estimation: NC 5.2
2. Phase estimation when φ may have more than t digits (approximation with error): NC 5.2.1 (Non-examinable)
3. Additional references RdW Ch4, G Ch9
4. Order finding and factoring NC 5.3, RdW Ch5, G Ch10

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information Cambridge University Press (2010)

RdW ≣ Quantum Computing Lecture Notes, Ronald de Wolf, https://arxiv.org/abs/1907.09415

G ≣ Introduction to Quantum Computation, Sevag Gharibian, Lecture notes.

Number Theory

1. Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2010) [Appendix 4]
2. Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons (1991)
3. Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (2008)

Probability of hypothesis H1 and H2 (Non examinable)

1. Ronald de Wolf, Quantum Computing: Lecture Notes, arXiv:1907.09415v1 (2019) [Footnote page 36].
2. See also Nielsen and Chuang [Chapter 5: page 233].

Public Key Cryptography and RSA

1. Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2010) [Appendix 5]
2. Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (2008)